EXHIBIT 48

UNITED STATES SECURITIES AND EXCHANGE COMMISSION

In the Matter of)

) File No. C-08755-A

SOLARWINDS)

WITNESS: Timothy Gordon Brown

PAGES: 312 through 584

PLACE: Securities and Exchange Commission

175 W. Jackson Blvd

Chicago, Illinois

DATE: Wednesday, March 9, 2022

The above-entitled matter came on for hearing, via WebEx, pursuant to notice, at 9:27 a.m.

APPEARANCES

On behalf of the Securities and Exchange Commission:
LORY STONE, ESQ.
WILLIAM BRAD NEY, ESQ.
BENJAMIN BRUTLAG
KENNETH ZAVOS
MARGARET VIZZI, IT Forensic Staff
ERA CALHOUN, Paralegal
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
(202)551-4500

On behalf of the Witness:
JULIE RIEWE, ESQ.
ANNA MOODY, ESQ.
JONATHAN DEMARS, ESQ.
Debevoise & Plimpton
801 Pennsylvania Avenue NW
Washington DC 20004
(202) 383-8000

CONTENTS

CONTENTS(CONT.)

PROCEEDINGS

MS. STONE: So we'll go ahead and go back on the record at 9:27 a.m. on March 9th, 2020. I am Lory Stone and with me from the Commission are Brad Ney, Benjamin Brutlag, Margaret Vizzi, Ken Zavos and Era Calhoun. We are officers of the Commission for the purposes of this proceeding.

We are today resuming the testimony of Tim Brown in the matter of SolarWinds, Inc., C-08755. Would counsel for the witness please identify themselves for the record?

MS. RIEWE: Julie Riewe, Anna Moody and Jon DeMars from Debevoise & Plimpton and Jason Bliss and Becky Melton from SolarWinds.

MS. STONE: This testimony is pursuant to a Commission subpoena which has been previously marked as Exhibit 144.

(SEC Exhibit No. 144 was previously marked.)

MS. STONE: Mr. Brown, do you understand that you remain under oath?

THE WITNESS: Yes.

Whereupon,

TIMOTHY GORDON BROWN

was re-called as a witness and, having been previously duly sworn, was examined and testified further as follows:

MS. STONE: And let the record reflect that a

I'm sorry, Exhibit 166 because I believe this is Confluence -- a Confluence report.

(SEC Exhibit No. 166 was marked for identification.)

Q So Exhibit 166 is an email from Confluence to Timothy Brown dated July 22nd, 2020. Its first Bates is SW-SEC-00001139.

Mr. Brown, do you recognize Exhibit 166?

A Let me read this.

(Brief pause.)

A Yeah.

Q What is it?

A I believe this is the -- a snip from the Confluence page associated with this incident with the notes of internal investigation and timelines and other things that went on.

Q And is this -- oh, I'm sorry, what were you saying?

A Oh, just in details associated with that incident.

Q Okay. And did you say that this -- did you confirm that this is related to the DOJ incident?

A Yes.

Q All right. I showed you the other exhibit first because I actually don't see -- oh, well, I don't see a date

here as to when SolarWinds was alerted. It looks like in the summary on the first page of this exhibit it talks about when the Department of Justice was first alerted. Do you see that? It says "May 28th, 2020?"

A Yeah. They first got alerted on 28th of May 2020 so I don't know when they alerted us. I would think it would be soon after that.

Q Okay. Can you just tell me a little bit about this Confluence report? It says at the top "Harry Griffiths created a page." How did this come into being?

MS. RIEWE: I think maybe, did you say this is a snip from the --

THE WITNESS: I believe this is a copy of the Confluence page. Confluence is a -- yeah, basically a tool we use to store information, data. This looks like this was a snip from our Confluence page.

BY MS. STONE:

Q And it's being emailed from Confluence to you. How frequently does that happen? Is that -- for the DOJ incident, would that -- it looks like it has an ITOM number. Would you get an email every time there's a change to the ITOM -- the associated text? Or how does it work? How do the emails, the ITOM emails work?

A Yeah, basically in Confluence you can up -- you can request that you get change requests and you can get

informed when changes occur in certain areas. So I don't know why this one specifically came through to me but it's common to get notified.

Q Okay. And is it correct that Harry Griffiths created this page? It says that at the top.

A Yeah, that's what it says.

Q Does that mean he's responsible for the content?

A Not all of the content. That means he is -- he created the page.

Q Where would he get the content?

A So a number of this could have -- again, it doesn't tell us where the incident was reported through. This doesn't have those details. This has details of what they told us but it doesn't have details of where it came in. So it could have come in through support, it could be a support ticket so some of the information could be from the support ticket. Some of the information -- so the information could be gathered from DOJ, from -- you know, entered from an email from DOJ. So I can't say that all this content is created by Harry.

Q Okay. All right. So I'm just going to direct your attention to some specific entries in Exhibit 166 and just see if you can tell me about them.

So let's go first to the page ending in 1141.

(Brief pause.)

Q So I think the fifth bullet down from the top under notes says, "this is a sophisticated attack on the DOJ. It mimics the behavior of our software with how we communicate the website structure and use XML files similar to how we communicate." And then there's two different iterations of something.

And then down below it says, "SolarWinds internal investigation," and there's some information there. And there's a bullet about halfway down the page that starts, "what we are seeing." Do you see that?

A Yes.

Q "What we are seeing is traffic going to this malicious site then doing a GIT to pull down something called Apollo from this" and it looks like an API website. And then it's followed by website "theme.com."

Do you know who conducted the SolarWinds internal investigation as it's described here?

A Yeah. So first off this was -- and somewhere in here I'm sure you see that this was a unique instance. This was a concerning incident because what our belief was is that -- so the OIP server that's talked about is our internally-hosted server, right? That's what OIP is. It's not -- it's something inside of our environment. It's not a product we sell, it's not a solution that is, you know, offered to customers or anything like that. The OIP server

sits inside of our environment and it takes information from clients to essentially improve their product. But it's a separate application, not something that's commercial. It's something that's inside of our environment to talk to.

What was the unique component of DOJ which got us concerned is that the traffic going to that environment looked like a piece of, you know, additional software that was installed on the machine that was targeting SolarWinds. It was targeting our back-end environment by doing this. So a lot of context around this is looking at, hey, did we harden the OIP server? Is it suspect to attack, is somebody trying to get into the SolarWinds back-end through this? So a lot of the traffic you'll see is what were they trying to do with this? They were mimicking our protocol which is very interesting. That means the threat actor did work in order to, you know, mimic our protocol and to try to make it look like OIP traffic.

So our theory with this is that somebody had -- again, we don't control the box that Orion is installed upon so our theory here is that, at this point in time was that somebody had either the box that they installed on was a dirty box and had this here, or that, you know, the box itself had been compromised without us and that that installed component was attacking SolarWinds with that OIP layer. So that's why you'll see a lot of hardening on OIP.

Q So thank you for that background. I just want to ask a couple of additional questions.

A Yeah.

Q Did you in fact determine whether the OIP server had been hardened?

A So we saw no signs of it being targeted, we saw no signs of our database being corrupted. We essentially brought in everybody to look at this traffic and this incident. So we brought over architects from other products. You'll see Chris Erway mentioned there, normally a Cloud architect but very good, strong technical mind. We had Tim Danner, the host of the -- you know, one of the architects who really built Orion from the back-end. So this -- but the fact that somebody was mimicking our traffic was a major sign that someone did research on us. That's why you'll see us calling out in other documents that, you know, people are doing reconnaissance on us. That means they were studying us, they were studying what our products did hence to be able to mimic that traffic. That's why this was such a memorable and different and unique incident that we'd never seen anything like this type of thing before.

Q So if you were -- if you were concerned that someone was doing research on SolarWinds that makes me think that you were concerned this was broader than just the DOJ, is that correct?

A Well, the fact was that someone was doing research. It wasn't a concern, it was a fact. In order to mimic our protocol you had to do research. You had to install product, you had to be able to test the product, you had to be able to find out what our protocol looks like. So it was a fact that they were -- that someone was doing research.

But in the case of DOJ, it was the only time we'd ever seen this. Remember, we had -- have, you know, thousands of downloads of these products and this was the only time we ever saw traffic like this at all, anywhere. So when we say is it unique to that environment? You know, from our point of view at that time, yeah, it was very unique to that environment because we had never seen anything like this before.

Q Okay. But just so I'm clear --

A Yeah.

Q -- it wasn't specific to DOJ, it was about mimicking SolarWinds?

A So just because it was at DOJ didn't matter, right? DOJ as a customer was not as much of a concern as our traffic is being mimicked from the outside. If we had seen that at anybody it would have been a concern. But DOJ as a customer was not as a -- yeah, it was not as much of a factor as the uniqueness of the -- what was found.

Q I guess my point though is if there's a -- if there's a threat actor that's doing research on SolarWinds, were you concerned that this could impact other customers?

A Yeah, of course. That's why it was treated so greatly, right?

Q Tell me again about the treatment. I think you said you brought in -- you brought in everyone to look at it. Tell me about that process.

A So very, very high priority. We're looking at all the details of it, we're looking at every aspect of our back-end OIP service to see whether it got corrupted, whether there were any issues in the OIP service. The OIP service, again not something we ship to clients, not something we ship to customers. But very -- something that we had to look at. So we looked at there, then we looked at the protocol, we looked at what was being used. We were actually able to determine the protocol didn't match the version of Orion that was there. The protocol was from an older version. So very different from a -- approach.

So what our concern was that we were being attacked by a threat actor, that SolarWinds was under attack in this way.

Q What did you make of the fact that the protocol didn't match Orion? Actually I wanted to --

A Yeah.

Q -- talk about this X Trace header that's in --
A Yeah.
Q -- that's in the same exhibit, Exhibit 166. Is that what you're referencing when you say protocol?
A Right, correct. In the entire protocol. But that, the X Trace header was from a different version of Orion than what was present. That's why, it targeted us to think that, okay, this must be a piece of malware that was created based on an old version of malware that got inserted into this server. So a separate complete component was inserted into the server.
Q Can you draw any conclusions from that about the capabilities of the threat actor?
A Just that the -- they had -- again, so our products are not -- don't require consulting. Our products don't require somebody to contact the sales person. Our products don't require a lot of heavy lifting to be able to test, right? We pride ourselves on simple, powerful and affordable products. People can download, try and buy them. So when you look at that aspect from what does it take to get one of our products and do reconnaissance on it, it takes, you know, an email address which is very good for what we do. It is, you know, what we do from a high volume sales product. Nothing wrong with it, it simply is -- takes a barrier away.

So a threat actor can do reconnaissance. So what this showed is that somebody did reconnaissance, somebody was doing investigation of a product, they were able to mimic a certain level of protocol from a certain version of Orion. And then they were able to utilize that OIP traffic and regenerate that OIP traffic going to again attack SolarWinds.
Q Okay. So you told me -- we started down this road but I think we got sidetracked a little bit.
You told me you brought people to -- you told me SolarWinds brought people together to look into the issue.
A Yep.
Q Was there anything else that was done?
A So we mobilized the architecture team, we informed people across -- you know, across the organization. We treated this as a, you know, very serious incident. We investigated the farest points that we could to get information from DOJ. We never got a server, we requested a server from them or a copy of the server. That would have helped us identify even more. But we followed our process but then we also did extra levels of investigation in the investigation stage, you know, by bringing people across the organization together. So we pulled off our Cloud architect, for example, Chris Erway, and brought him to look at the communications and the protocols and understand that.

So we really did mobilize a lot of different people in order to do that, in order to do the investigation associated with it.
Then it followed the normal process of incident response attempting to gather additional information, additional intel, you know, to determine what went on and how things happened. And then if I recall correctly, the DOJ just essentially went dark on us so they didn't respond to us any longer from requests.
Q All right. So you investigated internally using individuals from across the enterprise. Did you hire any third parties to review or --
A No. It was so specific to our environment that a third party would not help us with that.
Q Okay. Anything else that you did to investigate beyond what you've told me?
A We hardened the -- hardened the OIP server, again that --
Q What does that mean?
A It's our internal OIP server, right? It's not something we sell again but it's what we use. And that was --
Q When you say hardened -- sorry --
A Yeah.
Q -- when you say hardened, what does that mean?

A Yeah, that means we look at it, we look to see if there's anything in play that we could do to, you know, make it more resilient to attack. I believe we did network controls around the outside with our F5's to be able to stop unknown traffic to it. We looked at the code associated with it, I believe we had some -- so different teams build services like a business service in our -- and build products. So when we build a product for sale it goes through a number of the processes that we talked about before. But when you build a product for internal use, not a product but a service that you're going to use internally,, that doesn't necessarily follow the same processes that when we build the products from the outside.
But we implemented a number of those processes around the OIP server and investigated the server itself and then, you know, made some changes to the OIP server to make sure that -- you know, that it was hardened against attacks. Although we couldn't tell what the attack was from the data we had, essentially looked everywhere we could and put as many safeguards in place on the OIP server so it wouldn't affect us.
Q Okay. And why did you have to harden it? Why wouldn't -- why did those controls such as the network controls to stop unknown traffic, were they not in place before?

A You know, the hardest server is the server that's under the ocean that has no connectivity to anything. That's the ultimate hardened server, right? Then you start saying, well, I need to have the server talk to somebody. Okay, now you're vulnerable, right? So how do you make sure that it is as hardened as possible? Again, it's our own internal server, right? It's our own internal model to collect data from customers but not something we -- not something that we, again, sell or do anything like that to.

So yeah, there's levels of hardening that you can do and, you know, if the server functioned fine, the server worked fine, nobody would attack our OIP server for any reason that we could think of. It doesn't -- you know, it simply has some data in it from customers to help them. So it's really a helping server. Not like it has financial data, it's not like it has, you know, sensitive customer data, it's behind our DMC so it's not connected to anything. Can't use it as a jump-off point. So it becomes -- it's a interesting server but it's not an attack server. It's not something somebody's going to target for attack therefore we didn't believe it would be targeted for attack. Therefore that's why we had to go back and harden it after the fact.

Q Okay. And you said that your investigation didn't reveal evidence of an attack, is that right?

A The investigation didn't show any compromise of

the OIP server or the database associated with the OIP server. But the investigation did show that we could, you know, do some things to harden those interfaces in case the, you know, attacker was trying something that we didn't see. So this is all during that incident time, it's not post-incident.

Q I'm sorry, you cut out at the end. It's not --

A It is not post-incident, it's not what we know now.

Q Post-incident, okay. Yes.

A Right. It is the --

Q Understood, yes.

A -- point -- (garbled audio).

Q We're speaking as of summer of 2020?

A Correct.

Q Okay. You said the DOJ went dark on you. Who was communicating with the DOJ?

a I don't recall exactly who was doing emails and other things with the DOJ. It could have been Harry, it could have been one of the other incident response teams, it could have been support. But we were requesting information as we went through our investigation, we were requesting additional information to be able to do that. I'm not sure exactly the person who requested that information was.

Q Any idea why -- I assume when you say they went

dark on you, they just stopped responding. Is that accurate?

A Correct.

Q Any idea why?

A So often in these scenarios it can happen, right, where it's a priority for us because we think somebody's attacking our back-end. For them it's just another project, right? They stood up a server, okay, now let's go on. You know, we didn't get signs that they thought of this as serious. I believe we closed a deal with them the next month, that they bought more Orion. So yeah, for them it didn't -- was not as big of a deal as it was for us.

Q Are you speculating or do you know that?

A Don't know that, right? But again, they -- for us it was super important, for them, the amount of information that they shared with us was reasonable to start with. But going dark says it wasn't as -- for us it was critical, for them it didn't seem to be critical. And again, they did close a deal with us post-the-incident, bought more of Orion. Therefore, my summation that it wasn't as critical for them as what we thought for us.

Q Okay. I want to ask one more question before we move off from Exhibit 166. I'm still looking at 141.

There's a reference to website "theme.com" in a couple of different places. It says "connect" close towards

the middle. And then the sentence I read about, "we are seeing traffic going to this malicious site." Do you see the website theme.com address there?

A Yeah, website theme.com.

Q Are you familiar with that website?

A No. So I don't know the details of this. I know API.SolarWinds.com/swift is our OIP server but I don't know what the specific web theme is.

Q You don't recall having seen it before?

A I don't think it was relative to -- yeah, the details were -- yeah, somebody was trying to mimic our traffic. It wasn't -- details of exactly what didn't matter.

Q Okay. All right. So let's turn back to Exhibit 168 that we looked at briefly a few minutes ago.

And this is the exchange where it begins with Thomas Vrabel --

A Yeah.

Q -- sending a summary email, a background summary email. Just checking to see if we've talked about Mr. Vrabel before. I don't think so. Can you tell who Mr. Vrabel is?

A Yeah. Thomas is on our engineering team for Orion. He was one of the people that were involved in looking at this along with a few -- the people that are also

on this list.
Q Okay. And he's sending the email to Paul Gray who we've discussed. Who is Chandrasekhara Yerasi?
A Chandra is also on our engineering team. I believe he is one of the architects, I'm not sure exactly for what.
(Brief pause.)
A Oh, okay. Chandra moved to MSP. Okay. So Chandra may have been in a different organization so I'm not sure exactly.
Q Do you know if Chandra was in MSP as of the date of this email, so as of --
A I don't recall.
Q -- June 2020? Okay.
All right. So we've already discussed the background from Mr. Vrabel and you've confirmed that that was the DOJ incident we've been discussing.
In that same email Mr. Vrabel writes -- hold on just a second. Okay. So he writes, "as part of the background we're now dealing with the customer." We've already got that part.
The next paragraph he writes, "however during our analysis I found out that OIP server is using vulnerable library" followed by DLL site in version -- followed by a version number. There is a public CBE and he links a NIST

web address.
A Yep.
Q And then he writes, "this raised strong suspicion that OIP server is not under SDL." Is SDL a reference to the secure development lifecycle that we discussed yesterday?
A Yes.
Q What does that mean? What does Mr. Vrabel mean when he says "this raises a strong suspicion" --
A Right.
Q -- "that OIP server is not under SDL?"
A Yeah. So as I said before, that products are generally under SDL, right, the products that we build, the products that we sell to customers are under that process.
Q Uh-huh.
A And some of the other components that are built through our Bizapps team, so not by necessarily the engineering team but the IT function, we're not going through that SDL process.
Q Say that -- say that again for me. You said products are generally under SDL but some products by engineering are not?
A So, no. Products are under SDL, products that we ship are under SDL. Products that customers get are under SDL. We have a number of internally built solutions, we'll

call them solution, that do things like support our billing, that help us manage our customers, that help us generate lists of customers to send emails to. So these are called Bizapps, business applications. One of those business applications is OIP. That business application was built internally for the specific purpose of collecting information and helping customers with their deployment. So it doesn't -- that system is what Thomas is pointing out is -- as an engineer he's saying, I don't believe that this was under the secure development lifecycle --
Q Okay.
A -- therefore we should put it under that.
Q Is there a clear line, all products that go to customers are under SDL, all Bizapps are not?
A Not that clear of a line, right? We've been working to get all of the products that are built by Bizapps under SDL, they're just different. A number of the products built under Bizapps are built with salesforce.com, right? We build custom applications with salesforce.com. This one isn't but they have a different set of testing, different set of requirements around the outside of it. But at this point in time this was not under SDL. Therefore what we did was do evaluation on it and bring it under SDL.
Q Okay. And you said, "we are working to get all products in Bizapps under SDL." Why do you want all

products in Bizapps under SDL?
A Just to -- as a good practice, right? So the products that are behind the scenes are -- we're protecting SolarWinds, right, for those products. We're making sure that SolarWinds products, SolarWinds Bizapps, business applications are as resilient as possible by using the same best practices we're using on products, we're using with our internally-developed applications that we use for internal purposes.
Q Okay. When did the work begin to move all products in Bizapps under SDL?
A Ongoing, right. It was part of it. It was just primarily to start with the prioritized products first and then move towards doing more and more of it with Bizapps, business applications.
Q Do you recall generally when you started doing more with the business applications?
A I'd have to go back. I think we introduced SDL in 2018, I believe we said, so probably 20 -- yeah, 2019, 2018, 2019, somewhere in that range, but we'd have to look at data.
Q What does it mean if -- you've given me general responses but if you could be a little bit more specific. What does it mean if SDL is not enforced for OIP?
A What does it mean from what perspective?

companies.

So there's plenty of literature based on the SVR models that have been utilized.

MR. NEY: And would you agree that good cyber hygiene helps avoid being -- or helps companies avoid being impacted by those types of cyber attacks?

THE WITNESS: Yeah. This was not a cyber hygiene attack. This was a sophisticated attack that was extremely well planned, well thought and well executed. And you know, that's what a lot of the research has shown for this attack. So I don't consider this a hygiene attack.

MR. NEY: Okay. No other questions.

MS. STONE: All right. Why don't we take -- go off the record, take five minutes, and then we'll come back and wrap up.

So off the record at 5:22 p.m.

(Off the record.)

MS. STONE: We're back on the record at 5:29 p.m.

Mr. Brown, if you could just confirm there were no substantive conversations between yourself and SEC staff during the break?

THE WITNESS: Yep, confirmed.

MS. STONE: Okay. SEC colleagues, any further questions?

(No audible response.)

MS. STONE: All right. Mr. Brown, we have no further questions at this time. We may however call you again to testify in this investigation. Should it be necessary we will contact your counsel.

Before we close the record do you wish to clarify anything or add anything else to the statements you have made yesterday or today?

THE WITNESS: No. No.

MS. STONE: Counsel, do you wish to add -- wish to ask any clarifying questions at this time?

MS. RIEWE: No.

MS. STONE: All right. We are off the record at 5:30 p.m. on March 9th, 2022.

(Whereupon, at 5:30 p.m., the examination was concluded.)

*****

PROOFREADER'S CERTIFICATE

In the Matter of: SOLARWINDS
Witness: Timothy Brown
File Number: C-08755-A
Date: Wednesday, March 9, 2022
Location: Chicago, Illinois

This is to certify that I, Christine Boyce, (the undersigned), do hereby certify that the foregoing transcript is a complete, true and accurate transcription of all matters contained on the recorded proceedings of the investigative testimony.

_____ _____

(Proofreader's Name) 3-22-2022

REPORTER'S CERTIFICATE

I, Jemima Nobleza Euell, reporter, hereby certify that the foregoing transcript is a complete, true and accurate transcript of the meeting indicated, held on 3-9-22, at Chicago, Illinois, in the matter of: SOLAR WINDS.

I further certify that this proceeding was recorded by me, and that the foregoing transcript has been prepared under my direction.

3-22-2022